

MANUEL D'UTILISATEUR

Mettre en place un canal SFTP

Version 13

Table des matières

1. Qu’est-ce que SFTP?

SFTP signifie SSH File Transfer Protocol ou Secure File Transfer Protocol.

Comme l’indique la première définition, SFTP fait partie de SSH ou Secure Shell. Il s’agit d’un remplaçant sûr pour l’établissement d’une session de terminal sur des machines UNIX. SFTP est le composant de ce protocole SSH qui assure le transfert de fichiers.

Un client SFTP se comporte comme un client FTP classique, où vous avez une vue sur les répertoires et les fichiers, et où vous pouvez déposer, extraire… des fichiers avec les mêmes commandes que FTP.

Contrairement à FTP, les ordinateurs Windows ne disposent pas d’un client standard. Vous devez donc pour cela installer du **software supplémentaire**. Il existe des clients software SFTP gratuits et payants. Les systèmes Linux proposent des packages standard d’une implémentation open source de SSH (OpenSSH).

SFTP est toutefois un tout autre protocole que FTP. Il est en effet protégé à l’aide de **techniques cryptographiques**, ce qui signifie que tout le trafic entre un client et un serveur est entièrement chiffré, depuis le processus d’identification jusqu’à l’envoi de fichiers. Étant donné cette protection, SFTP convient très bien à l’échange **sécurisé** de fichiers sur **l’internet**.

Il existe plusieurs conditions pour s’identifier comme utilisateur via SFTP.
Bien entendu, on dispose toujours d’un **nom d’utilisateur**.
À côté de cela, une paire de clés électroniques remplace le mot de passe au sens classique du terme. Cette paire de clés comporte **une clé privée et une clé publique**. La clé privée reste chez celui qui l’a créée et sera de préférence encore protégée par un mot de passe additionnel. La clé publique peut être envoyée à toute partie adverse qui souhaite identifier le détenteur de la clé privée.

Ce système ressemble étroitement au système X.509 (comme celui de la carte d’identité électronique) qui utilise des clés privées et des certificats. Les principes sous-jacents sont identiques, mais SFTP utilise rarement des certificats. SFTP possède donc son propre format de clés. Ces clés ne peuvent pas être achetées comme un certificat, il faut les **générer soi-même**. La majorité des clients SFTP disposent d’une fonction pour générer cette paire de clés.

Tout comme le client, chaque **serveur SFTP** dispose également d’une paire de clés. Lors de l’établissement d’une connexion avec un serveur, celui-ci transmettra sa clé publique (également appelée host key) au client. C’est alors à l’utilisateur final qu’il appartient d’accepter cette clé. À partir de ce point, la connexion sécurisée peut être établie et l’utilisateur peut s’identifier.

L’authentification sur le serveur SFTP se fait via le nom d’utilisateur et la clé publique.

2. Choisir votre certificat digital qualifié

Chaque fichier de déclaration que vous envoyez par SFTP doit être accompagné d'un fichier de signature. Pour générer ce fichier de signature vous avez besoin d'un certificat digital qualifié.

Plusieurs choix s'offrent à vous :

1. Le certificat de **signature** de votre carte d'identité électronique (eID) (http://eid.belgium.be/fr/)

2. Un certificat digital qualifié du prestataire de services de certification suivant :
   GlobalSign : PersonalSign 3 pro
   (https://www.globalsign.eu/personalsign/personalsign3-pro/)

Comme la procédure de demande auprès d'un prestataire de services de certification peut prendre plusieurs jours, nous vous recommandons de vous y prendre bien à l'avance.

Ce certificat digital qualifié sera utilisé pour 2 actions :

- Vous devrez charger la clé publique de votre certificat digital qualifié (portant l'extension .cer) lors de la création de votre canal SFTP sur le site portail de la sécurité sociale (www.securitesociale.be).

- Sur la base de votre certificat qualifié (extension .pfx ou .p12) et pour chaque fichier de déclaration (FI), vous devrez créer un fichier de signature (FS) que vous placerez sur le serveur SFTP avec le fichier de déclaration.



Remarques importantes sur le choix de votre certificat

Il est important, lors du choix d'un certificat digital qualifié, de tenir compte de la manière dont vous comptez créer vos fichiers de signature (FS) :

Vous pouvez créer vous-même votre fichier de signature, en utilisant par exemple OpenSSL, ou utiliser des programmes que des producteurs de logiciels ou vous-même auraient développé.

Procédure OpenSSL :

Si vous souhaitez créer le fichier de signature par le biais de OpenSSL, il est important de demander un certificat à votre prestataire de services de certification, à partir duquel vous pourrez ensuite exporter la clé privée. Ceci pose problème pour les certificats figurant sur des cartes à puce ou des clés USB.
En effet, la procédure décrite dans la partie 10 Annexe : Générer un fichier de signature (FS) via OPENSSL ne convient PAS aux certificats qui se trouvent sur une carte d'identité électronique (eID) ou sur une carte Isabel. Dans la pratique, la procédure ne peut être utilisée que pour des certificats émis par Globalsign.

Apposer sa signature avec la carte d'identité électronique (eID) :

Si vous voulez créer un fichier de signature avec l'eID, vous pouvez utiliser l'application **Belgian eID Signer** ou une procédure avec **Cryptonit**. Vous trouverez l'application Belgian eID Signer et la procédure avec Cryptonit dans la bibliothèque de documents complémentaires (https://www.socialsecurity.be/public/doclibrary/fr/batch.htm). Vous pouvez bien entendu développer vous-même les programmes nécessaires ou faire appel à des logiciels disponibles sur le marché.

Les procédures avec l'application Belgian eID Signer et avec Cryptonit exigent la présence du titulaire de l'eID. Pour chaque fichier de signature, l'eID devra être insérée dans le lecteur de carte et le titulaire de l'eID devra saisir son code PIN. Par conséquent, si le titulaire de l'eID est absent et que vous devez créer un fichier de signature pour l'envoi d'un message structuré, vous devrez utiliser une autre eID. Avant l'envoi, votre gestionnaire local ou co-gestionnaire local devra alors charger la clé publique de l'autre eID dans les paramètres de votre canal sur le site portail.



Apposer sa signature avec la carte Isabel :

Construire un fichier de signature sur base d'une carte Isabel **n'est pas possible** parce que la clé privée ne peut pas être exportée. Nous ne sommes donc pas en mesure de vous fournir un manuel ou une technique pour le faire. Le helpdesk de chez Isabel ne sait pas vous aider non plus.

3. Votre connexion internet

Pour transférer rapidement et correctement des fichiers via SFTP, il est primordial de disposer d'une connexion internet de qualité.
Vous avez donc tout intérêt à vérifier depuis quel PC ou serveur le transfert s'effectue le mieux. Évitez le chargement via une connexion internet sans fil. En effet, de petites perturbations dans le réseau sans fil peuvent rompre le transfert de fichiers.

Contrôlez également les paramètres de votre pare-feu. Ce dernier doit autoriser le trafic SFTP vers le port 8022.

Veillez aussi à disposer d'une bande passante suffisante durant le transfert. D'autres processus en cours peuvent occuper la bande passante nécessaire au bon transfert via SFTP.

4. Choisir votre client SFTP.

Pour pouvoir communiquer avec notre serveur SFTP, vous avez besoin d'un client SFTP.

Vous travaillez avec Windows:

Les ordinateurs Windows ne disposent pas d'un client SFTP standard.
Vous pouvez utiliser un moteur de recherche et effectuer une recherche sur 'SFTP Client'.
Vous trouverez, parmi les résultats, des clients software SFTP gratuits et payants.
Certains clients SFTP fonctionnent de manière manuelle, d'autres peuvent être automatisés.
Vous êtes libre de choisir le client qui correspond le plus à vos besoins.

Vous travaillez avec Linux:

Les systèmes Linux proposent des packages standards d'une implémentation open source de SSH (OpenSSH).

Vous travaillez avec Apple:

Il existe également plusieurs clients SFTP pour Apple. Vous pouvez les trouver par un moteur de recherche et effectuer une recherche sur 'SFTP & Apple' ou sur le site www.apple.com.

Documentation:

À titre informatif, vous trouverez dans la bibliothèque technique (https://www.socialsecurity.be/public/doclibrary/fr/batch.htm) de la documentation sur les clients SFTP manuels (Filezilla, WinSCP, Bitvise Tunnelier) que nous avons nous-mêmes testés.

5. Créer votre paire de clés

Pour effectuer un envoi via SFTP, vous avez besoin d'une paire de clés SSH. Vous devez la créer vous-même.
Dans certains clients SFTP est compris un générateur de clé.
Si le client que vous avez choisi ne dispose pas d'un générateur de clé, vous devrez créer les clés via un autre générateur de clés que vous pouvez trouver facilement via une recherche sur internet. Le programme Putty Key Generator fonctionne très bien. Vous pouvez le retrouver en utilisant « puttygen » dans un moteur de recherche.

Votre clé publique doit être chargée lors de l'ouverture du canal SFTP sur le portail de la sécurité sociale.
Votre clé privée doit être chargée dans le client SFTP que vous utilisez. Veuillez pour cette action consulter la documentation de votre client SFTP. Il est conseillé de protéger votre clé privée avec un mot de passe.

Spécifications:

Format
Une distinction est faite entre les clés qui sont compatibles avec la version 1 de SSH et celles qui sont compatibles avec la version 2. La version 1 est considérée comme peu sûre et ne sera pas acceptée.

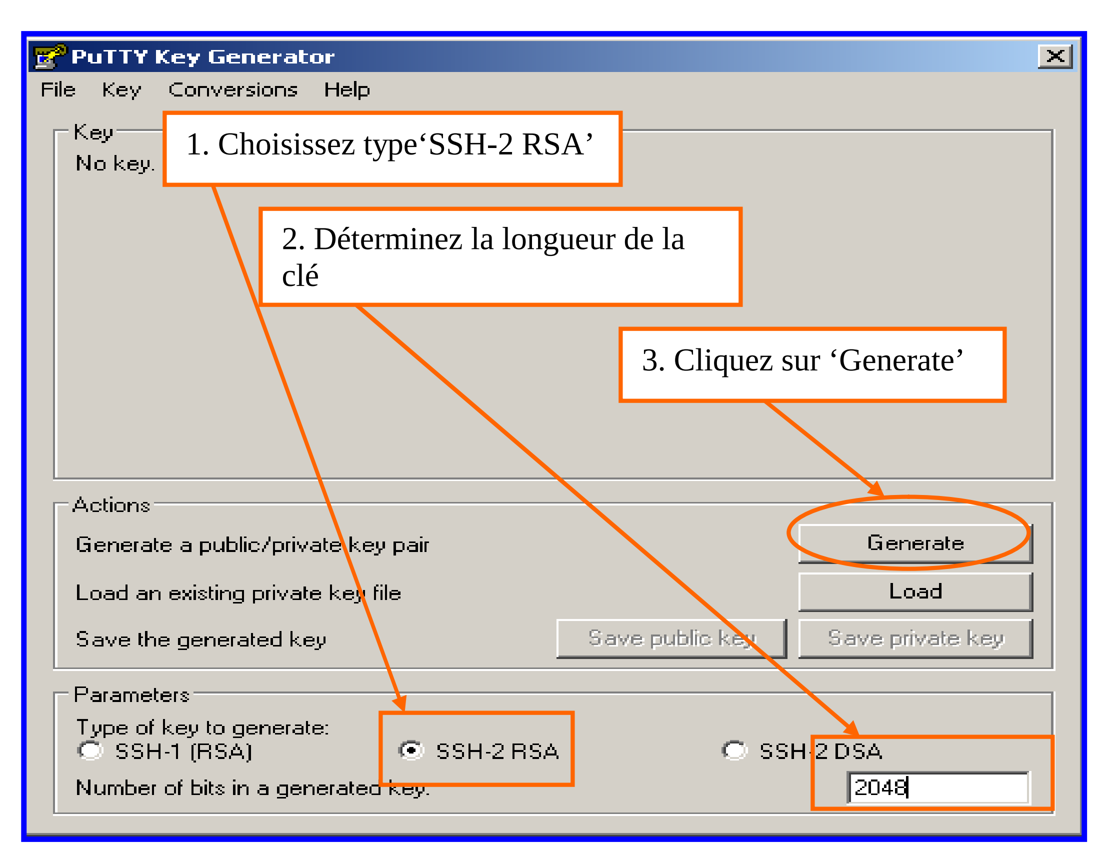
En plus il y a différents formats pour les clés publiques. Les plus courants sont ceux du logiciel OpenSSH et SSH. (La mise en application commerciale de SSH-protocol).
Pour les clés publiques, les formats de OpenSSH et de SSH seront soutenus uniquement.

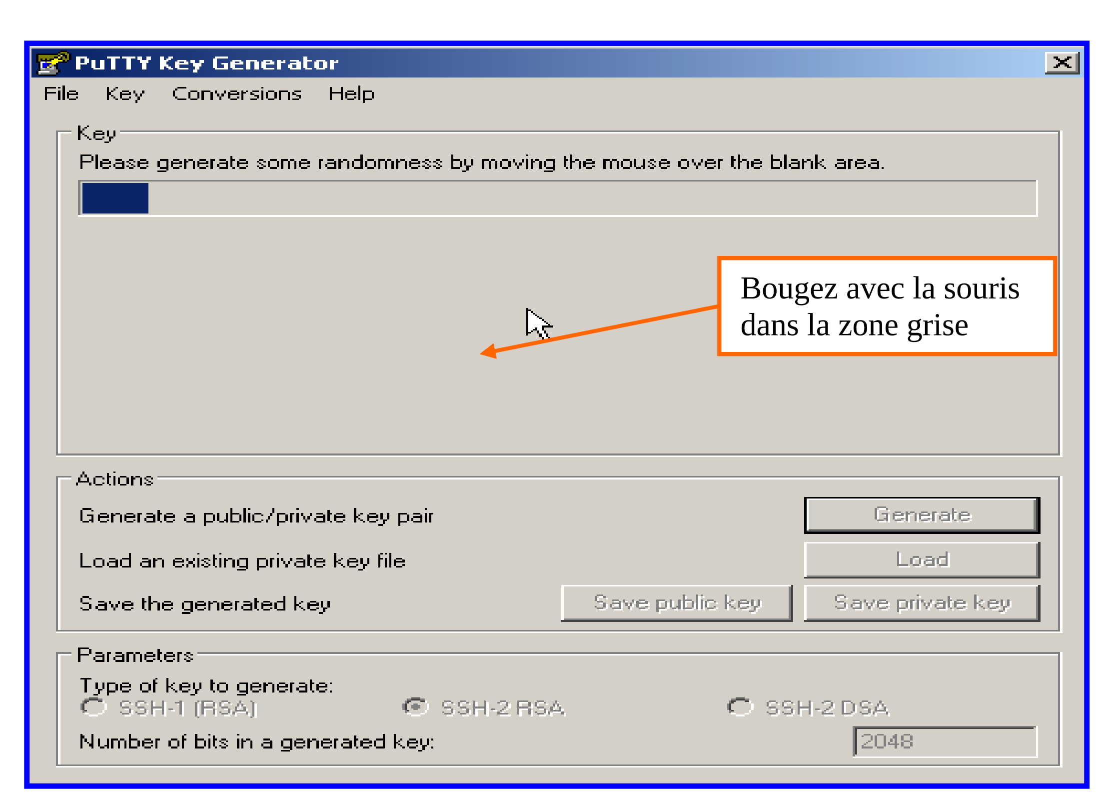
L'algorithme & la longueur
Lors de la génération des clés, vous devez faire attention au fait d'avoir choisi le type et la longueur correcte.
Il y a deux types possibles (RSA et DSA) dont seuls les RSA seront acceptés.
Comme longueur de clé, choisissez 2048 ou plus (3072, 4096). Les clés plus courtes ne seront pas acceptées.
Nous vous invitons à protéger votre clé privée par un mot de passe lorsque vous la sauvez sur votre machine.

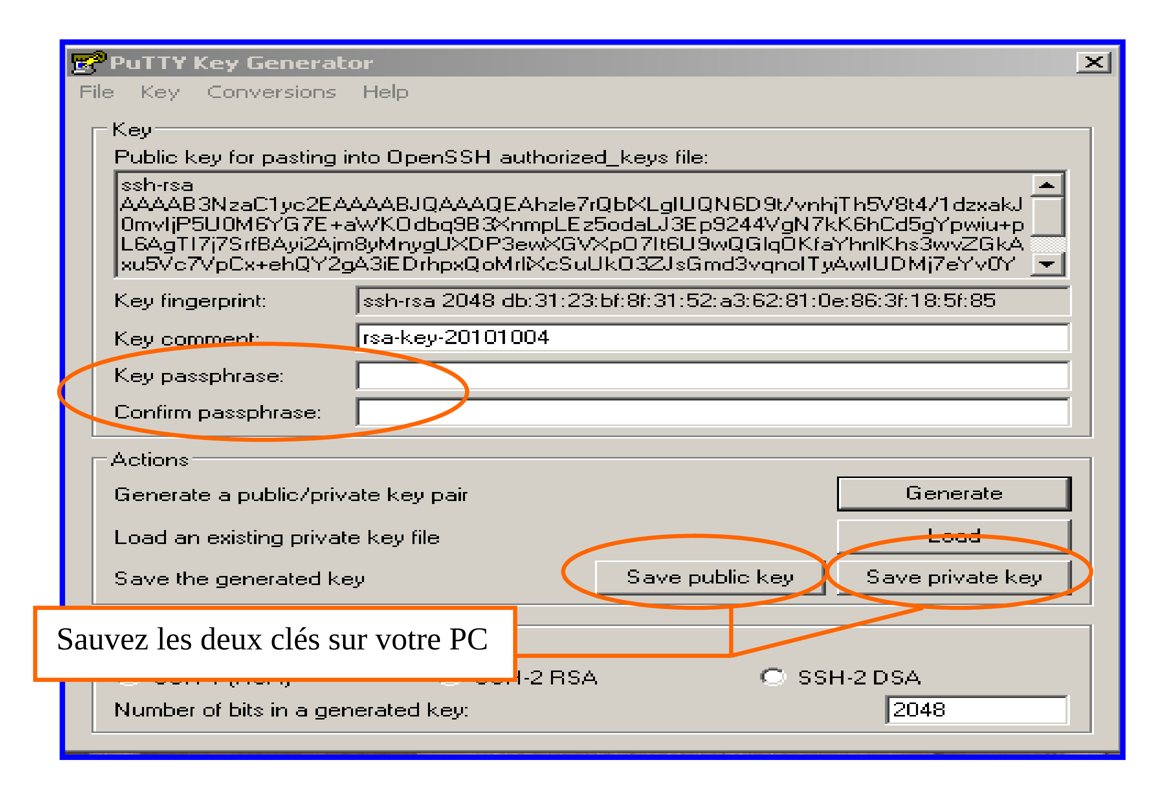
Bref résumé:

Les clés compatibles avec SSH v2
Les formats OpenSSH et SSH sont acceptés
Type de clé : SSH2-RSA
Longueur de clé : de 2048 à 4096 bits.

Exemple : création des clés avec Putty Key Generator







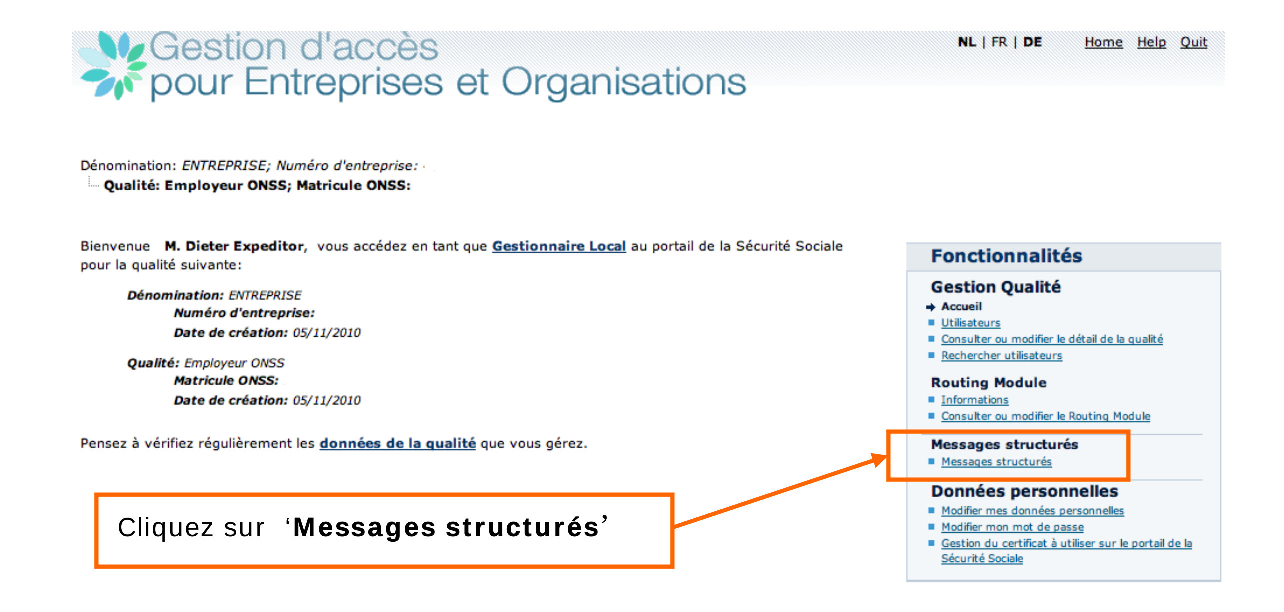
Il est conseillé de sauvegarder la clé privée avec un mot de passe. (Key passphrase) Certains clients SFTP n'admettent toutefois pas de fonctionner avec une clé privée qui est protégée avec un mot de passe.

Si vous avez créé votre clé avec votre client SFTP, référez-vous à la documentation de celui-ci.

6. Créer votre canal SFTP sur le portail de la sécurité sociale

Il n'y a que le gestionnaire local et le co-gestionnaire local de la qualité qui peuvent ouvrir un canal.

Ci-dessous, vous trouvez les différentes étapes que vous devez parcourir pour ouvrir votre canal SFTP. Si vous disposez déjà d'un canal d'expédition pour la qualité ou si vous avez eu pour la qualité un canal d'expédition dans le passé vous ne devez pas parcourir certains étapes.



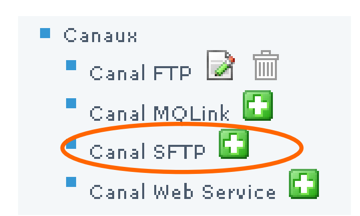
Gestion d'accès
pour Entreprises et Organisations

NL | FR | DE   Home Help Quit

Dénomination: *ENTREPRISE; Numéro d'entreprise:*
Qualité: Employeur ONSS; Matricule ONSS:



(*) Si un canal d'envoi existe déjà pour la qualité, cliquez sur l'icône à côté de SFTP dans la partie droite de votre écran sous « Messages structurés ».



Vu qu'il existe alors déjà un utilisateur technique, vous ne verrez pas les deux écrans suivants.

Gestion d'accès
pour Entreprises et Organisations

NL | FR | DE Home Help Quit

Dénomination: *ENTREPRISE; Numéro d'entreprise:*
Qualité: Employeur ONSS; Matricule ONSS:

Information > Personne de contact > Données du canal > Confirmation

Création d'un utilisateur technique

Outre la gestion des utilisateurs pour les applications du portail, il est possible de gérer des données relatives à l'envoi de messages structurés.

L'envoi de messages structurés (transfert de fichiers) est surtout utile pour effectuer des envois avec un grand volume de déclarations. L'échange de données par transfert de fichiers est actuellement possible via les canaux batch SFTP, FTP et MQLink.

Lors de votre première connexion pour demander accès aux échanges structurés, l'application vous demande d'enregistrer les informations nécessaires.

Annuler | Suivant

Cliquez sur **'Suivant'**



Gestion d'accès
pour Entreprises et Organisations

NL | FR | DE Home Help Quit

Introduisez les données de votre personne de contact technique et cliquez sur **'Suivant'**

Dénomination: *ENTREPRISE; Numéro d'entreprise:*
Qualité: Employeur ONSS; Matricule ONSS:

Information > **Personne de contact** > Données du canal > Confirmation

Création d'un utilisateur technique

Personne de contact pour les échanges de messages structurés par les canaux

Données d'identification

Nom * :
Prénom * :
Titre * : Mr
Fonction * :
Régime linguistique * : Français
Téléphone * :
Fax :
Mobile :
Adresses e-mail ** :

* Champs obligatoires
** Au moins une adresse e-mail

Annuler | Précédent | Suivant

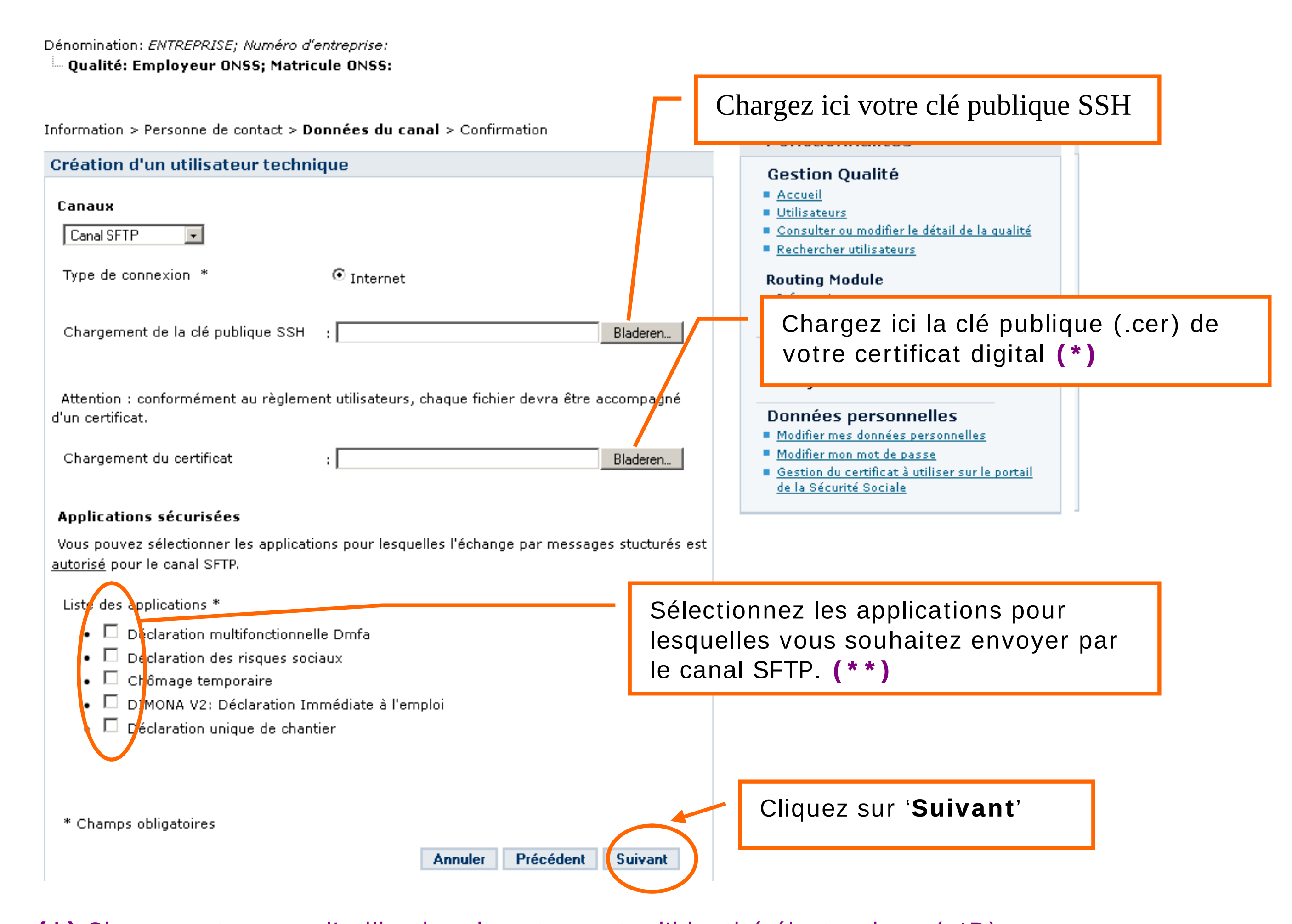
Fonctionnalités

Gestion Qualité
- Accueil
- Utilisateurs
- Consulter ou modifier le détail de la qualité
- Rechercher utilisateurs

Routing Module
- Informations
- Consulter ou modifier le Routing Module

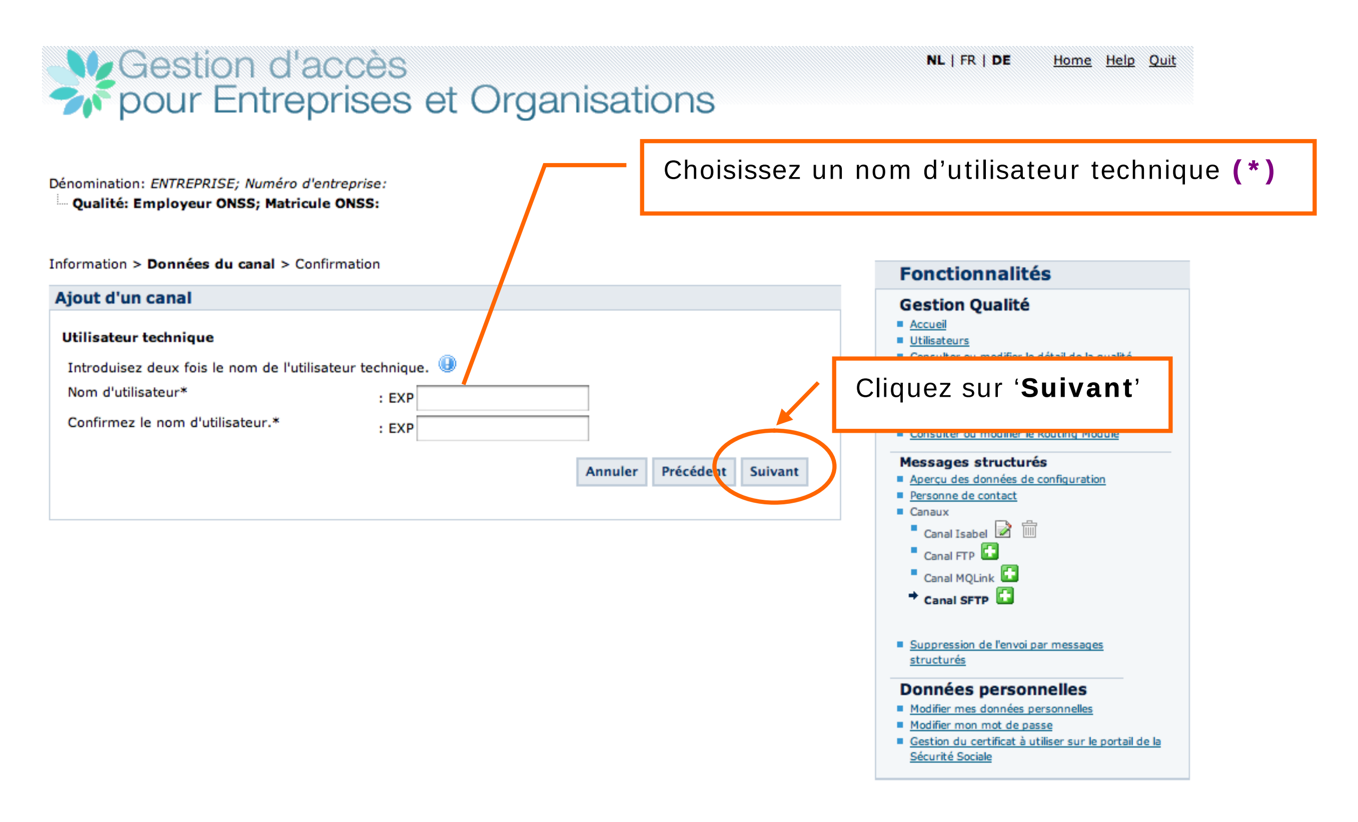
Messages structurés
- Enregistrement des données de configuration

Données personnelles
- Modifier mes données personnelles
- Modifier mon mot de passe
- Gestion du certificat à utiliser sur le portail de la Sécurité Sociale



(*) Si vous optez pour l'utilisation de votre carte d'identité électronique (eID), vous devez charger ici le certificat de **signature** de votre eID.

(**) Si vous disposez déjà d'un canal d'envoi pour la qualité et vous choisissez les mêmes applications pour votre canal SFTP, vous devrez indiquer un canal de préférence par application.



Caractéristiques d'un nom d'utilisateur technique :

- Minimum 8 – maximum 20 caractères
- Les chiffres (0-9) et les lettres de l'alphabet (a-z) sont admis uniquement
- Pas d'espaces
- Une fois créé, il n'y a plus moyen de le modifier
- Ne dois pas exister dans le système web de la sécurité sociale

(*) Si vous disposez déjà d'un canal d'expédition ou si vous avez eu un canal avec dial-up dans le passé, vous ne verrez pas cet écran et ne devrez donc pas choisir de nom d'utilisateur technique vu que le nom d'utilisateur technique choisi reste d'application pour SFTP.

Gestion d'accès
pour Entreprises et Organisations

NL | FR | DE   Home Help Quit

Dénomination: *ENTREPRISE; Numéro d'entreprise:*
Qualité: Employeur ONSS; Matricule ONSS:

Information > Personne de contact > Données du canal > **Confirmation**

Création d'un utilisateur technique

Personne de contact

Nom	: Expediteur
Prénom	: Didier
Titre	: mr
Fonction	: IT
Régime linguistique	: fr
Téléphone	: 025455078
Fax	:
Mobile	:
Adresses e-mail	: batch@eranova.fgov.be
	:
	:

Canal

Canal	: SFTP
Type de connexion	: Internet
Clé publique SSH	: chargée

Certificat

Propriétaire du certificat	: (Signature)
Nom de l'entreprise	: Not specified
Fournisseur du certificat	: SERIALNUMBER=200803, CN=Citizen CA, C=BE
Date d'expiration	: 26/03/2013
Numéro de série (format décimal)	: 21267647932558708165435772380
Numéro de série (format hexadécimal)	: 10 00 00 00 00 00 0b 7a 21 df 5c 29

Utilisateur technique

Nom d'utilisateur	: EXPDEMOENTREPRISE

Applications sécurisées

- Déclaration multifonctionnelle Dmfa
  - *canal préférentiel :SFTP*
- Déclaration des risques sociaux
  - *canal préférentiel :SFTP*
- DIMONA V2: Déclaration Immédiate à l'emploi
  - *canal préférentiel :SFTP*

Annuler | Précédent | Confirmer

Cliquez sur '**Confirmer**'

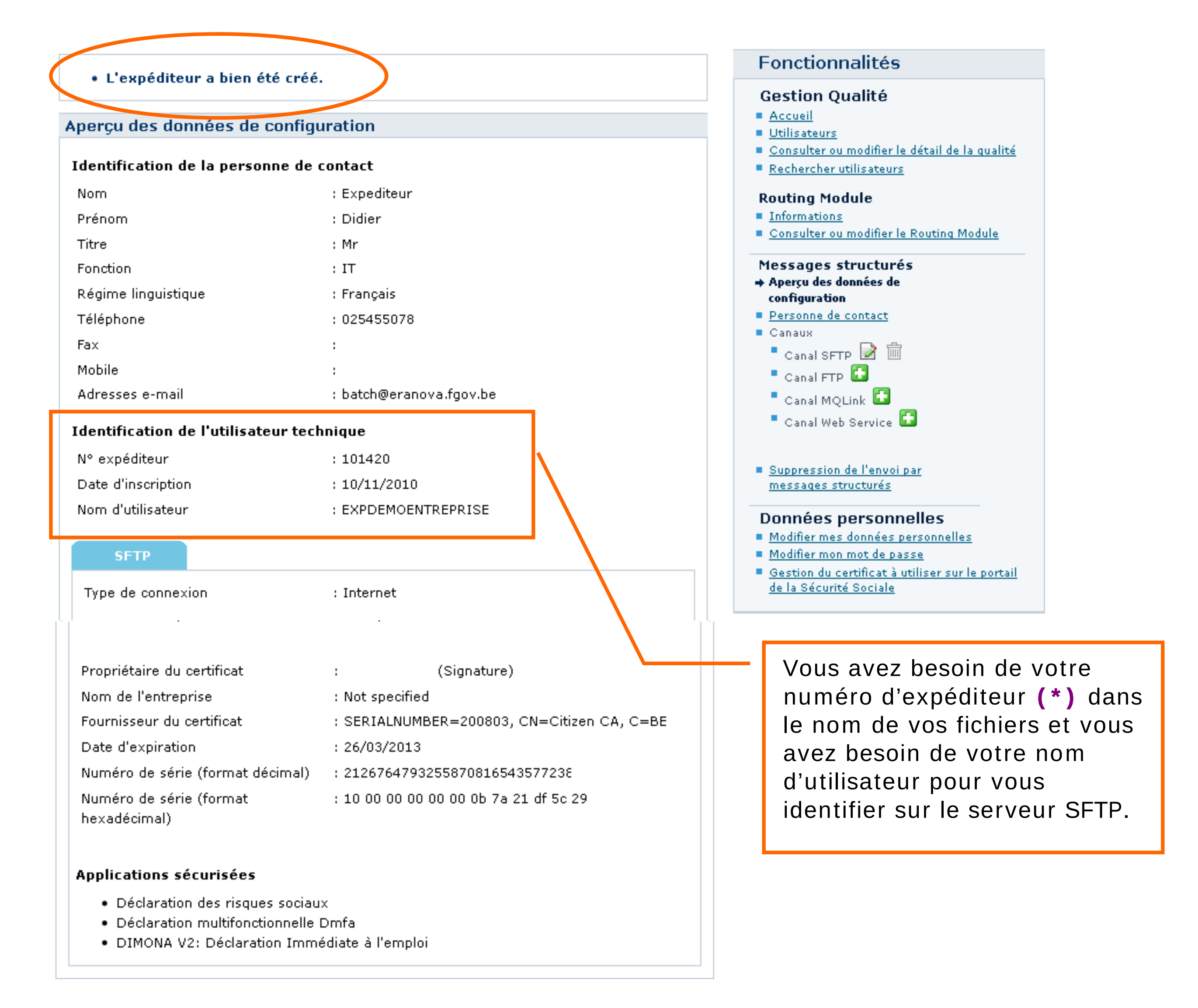
Fonctionnalités

Gestion Qualité
- Accueil
- Utilisateurs
- Consulter ou modifier le détail de la qualité
- Rechercher utilisateurs

Routing Module
- Informations
- Consulter ou modifier le Routing Module

Messages structurés
- → **Enregistrement des données de configuration**

Données personnelles
- Modifier mes données personnelles
- Modifier mon mot de passe
- Gestion du certificat à utiliser sur le portail de la Sécurité Sociale



(*) Si vous disposez déjà d'un canal d'envoi pour la qualité ou si vous avez déjà eu un canal d'envoi dans le passé, vous conserverez toujours le numéro d'expéditeur que vous aviez déjà.

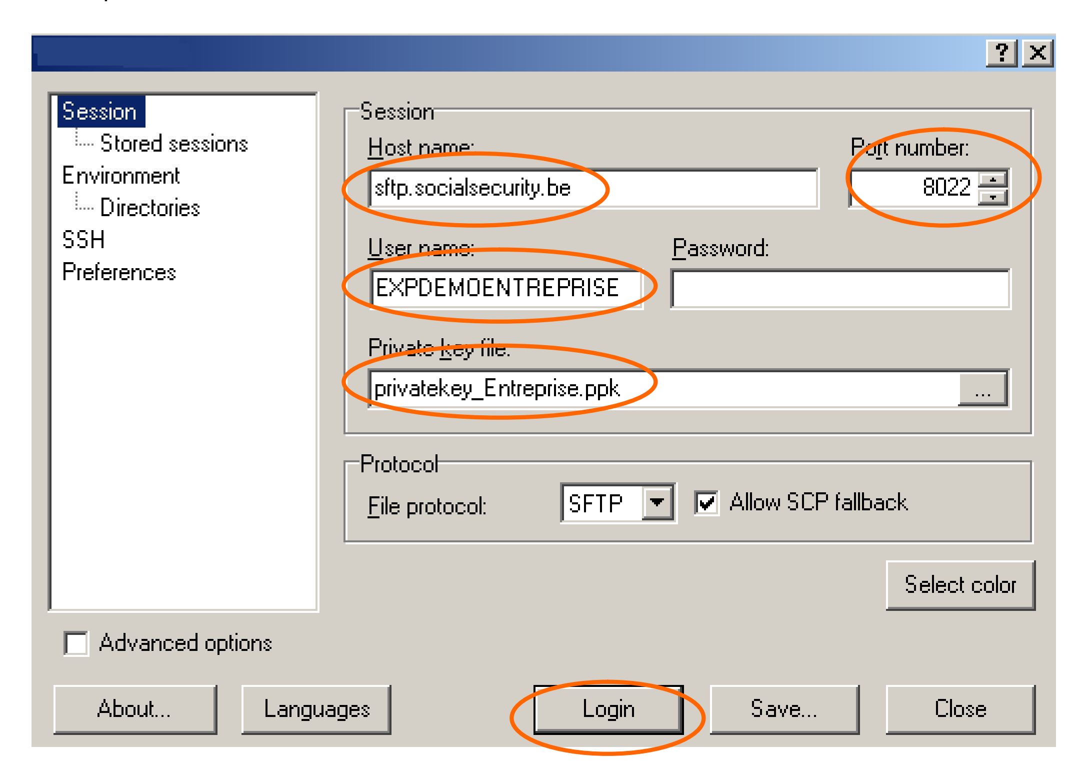
7. Paramétrer votre client SFTP

Pour faire la liaison entre le serveur SFTP de la sécurité sociale (host) vous devez introduire les données ci-dessous dans votre client SFTP (*).

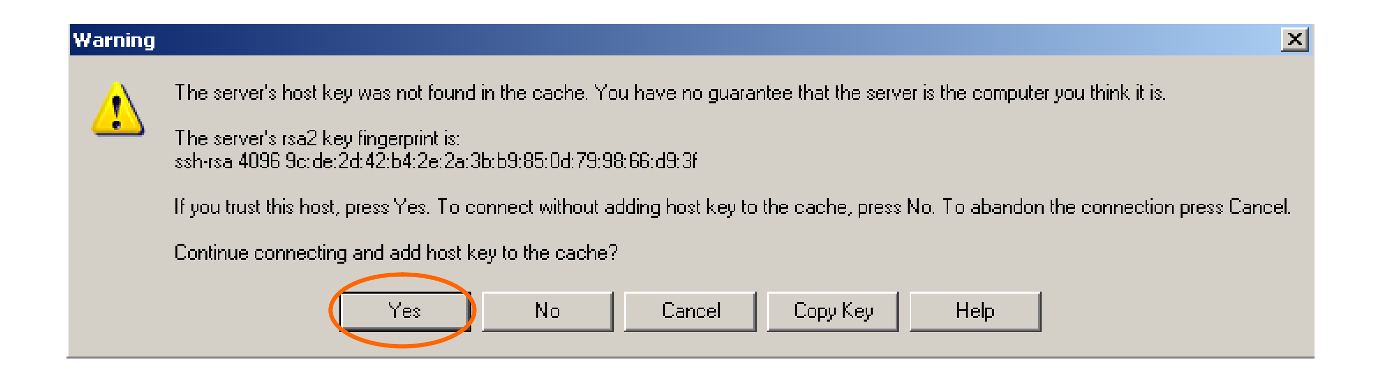
- Le nom du host est:'**sftp.socialsecurity.be**'
- Le numéro de porte est: '**8022**'. (Attention : il est possible que vous ayez à adapter votre pare-feu (firewall) pour permettre le trafic vers cette porte).
- Le **nom d'utilisateur** (commence par **EXP**) que vous avez choisi lors de la création de votre canal SFTP sur le portail de la sécurité sociale. (Si vous aviez déjà par le passé un nom d'utilisateur technique, il est possible que celui-ci commence par **UM**).
- Chargez la clé privée, que vous avez créée dans le générateur de clé, dans votre client SFTP.
- Lors de la première connexion vous devez **accepter** la clé publique (également appelée **host-key**) du serveur SFTP de la sécurité sociale
- Si vous avez protégé votre **clé privée** par un **mot de passe**, le client SFTP va le demander.

(*) Pour installer votre client SFTP, référez-vous à la documentation de celui-ci. À titre informatif, vous trouverez dans la bibliothèque technique (https://www.socialsecurity.be/public/doclibrary/fr/batch.htm) de la documentation sur les clients SFTP manuels (Filezilla, WinSCP, Bitvise Tunnelier) que nous avons nous-mêmes testés.

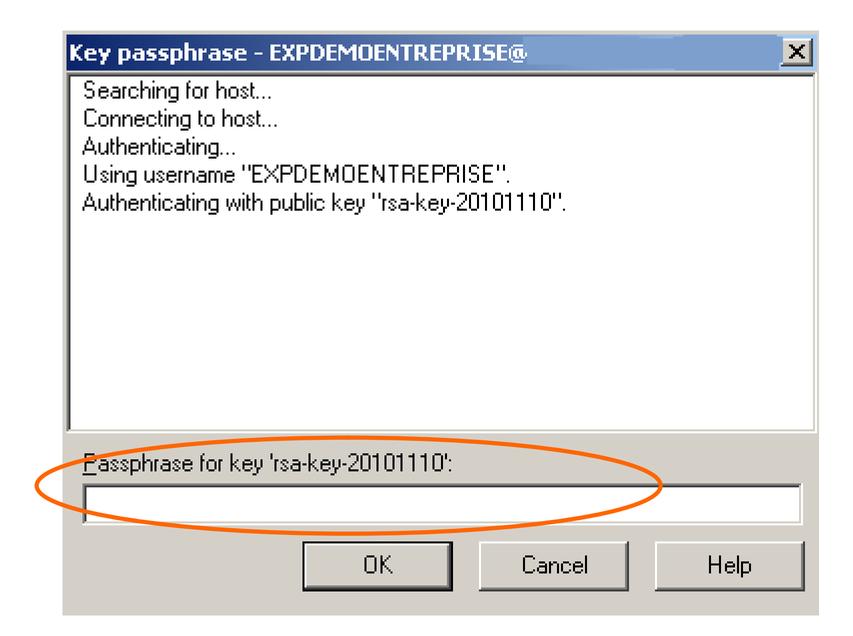
Exemple:



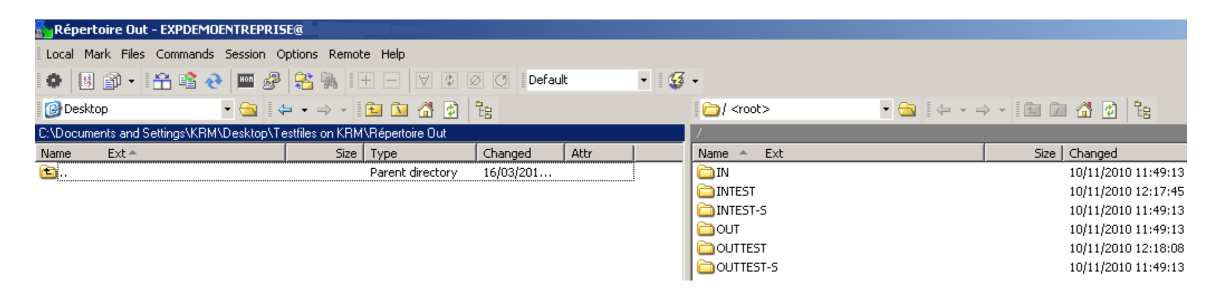
Acceptez une fois la clé publique (host key) du serveur SFTP de la sécurité sociale. Il s'agit de la clé publique du serveur : ssh-rsa 4096 9c:de:2d:42:b4:2e:2a:3b:b9:85:0d:79:98:66:d9:3f



Si vous avez protégé votre clé privée par un mot de passe, on vous demande de l'inscrire.



Ensuite, vous êtes enregistré. Vous voyez à gauche les répertoires de votre pc et à droite, les répertoires du serveur SFTP de la sécurité sociale.



8. Fichiers

Dans l'environnement de production pour SFTP vous devez ajouter, à côté de votre fichier de déclaration (FI), un fichier GO et un fichier de signature (FS) et les placer sur le serveur.

Le fichier de signature n'est pas exigé dans l'environnement de simulation mais le fichier GO, lui, est obligatoire.

8.1 Structure du nom des fichiers:

Pour les messages structurés, les noms de fichiers ont la structure suivante :

FI.XXXX.123456.20120213.00001.R.1.1
FS.XXXX.123456.20120213.00001.R.1.1
GO.XXXX.123456.20120213.00001.R.1
(TD.XXXX.123456.20120213.00001.R.1)

Première partie du nom:
FI Le fichier de déclaration
FS Le fichier de signature
GO Le fichier vide qui lance le traitement
TD Le fichier vide qui annule le traitement

Deuxième partie du nom:
XXXX : Le deuxième élément du nom du fichier décrit le contenu du fichier.

AOAT: pour une déclaration DRS "Accidents du travail"
DIMN: pour une déclaration Dimona
DMFA: pour une déclaration originale DmfA
DMRQ: pour une consultation (Request) DmfA
DMWA: pour une modification de DmfA
DUCN: pour une déclaration unique de chantier (DUC)
PFRQ: pour une consultation du fichier du personnel
TWCT: pour une déclaration de Chômage Temporaire
VBLV: pour une déclaration "Livre de validation"
WECH: pour une déclaration DRS "Chômage"
ZIMA: pour une déclaration DRS "Indemnités"

Troisième partie du nom:
123456 : Il s'agit du numéro d'expéditeur attribué à l'expéditeur lors de la création du premier canal pour sa qualité.

Quatrième partie du nom:
20120213 : C'est la date de création du fichier sous la forme AAAAMMJJ.

Cinquième partie du nom:
00001: Il s'agit d'un numéro **unique** de votre choix qui indique de manière unique le nom du fichier, par date de création et par environnement.

Sixième partie du nom:
Indique l'environnement de travail:
«**R**» Utilisé pour la production
«**T**» Utilisé pour un **test** (DRS, DUC, Dimona, Chômage Temporaire) ou un **test de circuit DmfA**
«**S**» Utilisé pour un **test de déclaration DmfA**

Différence test de déclaration (S) et test de circuit (T) DmfA

Avec la DmfA, vous pouvez envoyer vos fichiers de test comme test de déclaration (extension S et dossier INTEST-S) ou comme test de circuit (extension T et dossier INTEST). Pour toutes les autres applications, vous pouvez utiliser uniquement l'extension T et le dossier INTEST pour vos fichiers de test.

Lors d'un **test de déclaration (extension de fichier S)**, tous les contrôles de réception et tous les contrôles de contenu sont parcourus. Il n'y a pas de contrôle des données d'identification du/des travailleur(s). Après un ACRF positif, vous recevez une notification, mais pas de fichier DMNO ou PID. Vous placez vos fichiers dans le dossier **INTEST-S** et vous trouvez le résultat dans le dossier **OUTTEST-S.** Étant donné que la déclaration n'est pas sauvegardée dans l'environnement de simulation, vous pouvez tester plusieurs fois la même déclaration.

Lors d'un **test de circuit (extension de fichier T)**, le circuit de contrôle entier est parcouru comme dans l'environnement de production. Il y a un contrôle des données d'identification du/des travailleur(s),mais pas de contrôle d'identification via Sigedis. Après un ACRF positif, vous recevez les fichiers de réponse comme dans l'environnement de production (notifications, PID et DMNO).
Vous placez vos fichiers dans le dossier **INTEST** et vous trouvez le résultat dans le dossier **OUTTEST**.
En cas de notification positive, la déclaration est sauvegardée dans l'environnement de simulation. Tout comme dans l'environnement de production, le test de circuit est limité à une déclaration acceptée par combinaison numéro ONSS/trimestre.

Septième partie du nom :
1: Indique le nombre total de partie(s)
Une déclaration peut être composée de maximum 9 parties.
Les déclarations DRS et Chômage Temporaire ne peuvent pas être fractionnées donc il n'y a pas de septième partie.
Ex : FI.WECH.123456.20120213.00001.R

Huitième partie du nom:
1: Indique le numéro de la partie.
Les déclarations DRS et Chômage Temporaire ne peuvent pas être fractionnées donc il n'y a pas de huitième partie.
EX : FI.AOAT.123456.20120213.00001.R

Exemples:

- L'expéditeur envoie un morceau:

  FI.DMFA.123456.20120213.00001.R.1.1
  FS.DMFA.123456.20120213.00001.R.1.1
  GO.DMFA.123456.20120213.00001.R.1

- L'expéditeur envoie deux morceaux:

  FI.DMFA.123456.20120213.00001.R.2.1
  FI.DMFA.123456.20120213.00001.R.2.2
  FS.DMFA.123456.20120213.00001.R.2.1
  FS.DMFA.123456.20120213.00001.R.2.2
  GO.DMFA.123456.20120213.00001.R.2

8.2 Le fichier de déclaration (FI):

Les fichiers de déclaration (FI) sont identiques pour tous les canaux.

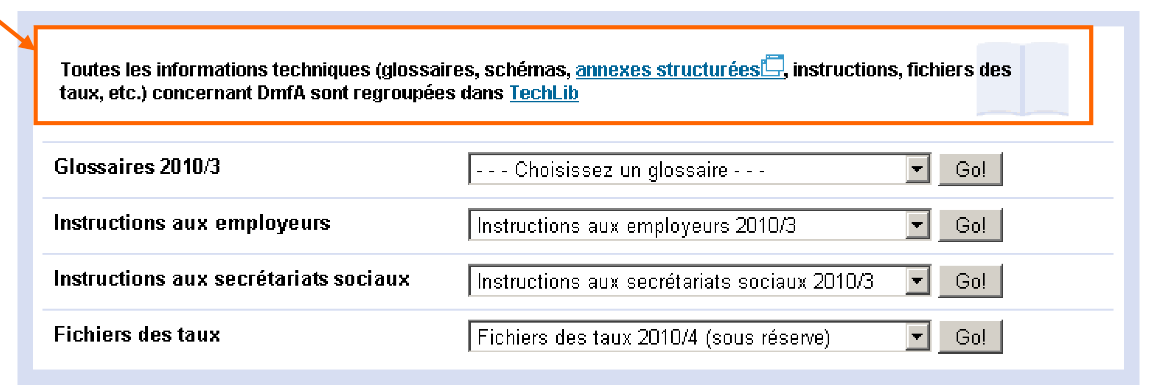
Structure du nom du fichier de déclaration

FI.application.numéro d'expéditeur.date.le numéro d'ordre.l'environnement de travail.le nombre de parties.le numéro de la partie
Ex : FI.DMFA.123456.20120213.00001.T.1.1

Sur la page de départ de chaque application sur le portail de la sécurité sociale dans la librairie technique, vous trouvez toutes les informations techniques (glossaires, les schémas, les annexes structurées et les instructions) pour faire votre fichier de déclaration.







8.3 Le fichier de signature (FS)

- Le fichier de signature comprend la signature électronique sur base de votre certificat qualifié.

- Vous pouvez utiliser les certificats digitaux qualifiés suivant :
  - GlobalSign : PersonalSign 3 pro (https://www.globalsign.eu/personalsign/personalsign3-pro/)

  - Le certificat de **signature** de la carte d'identité électronique
- Vous devez créer le fichier de signature avec le certificat que vous avez renseigné pour votre canal d'expédition.

- Vous pouvez créer votre fichier de signature (FS) vous-même, via par exemple, OpenSSL(*) ou vous pouvez utiliser un programme d'une maison de soft ou le développer vous-même.

- Pour OpenSSL(*), il est important que votre certificat ne se trouve pas sur une carte à puce ou une clé USB pour que vous puissiez exporter la clé privée.

- **Si vous voulez créer un fichier de signature avec l'eID, vous pouvez utiliser l'application Belgian eID Signer ou une procédure avec Cryptonit. L'application et la procédure se trouvent dans la bibliothèque de documents complémentaires:** (https://www.socialsecurity.be/public/doclibrary/fr/batch.htm).

- Lorsqu'une déclaration (FI) est transférée en différentes parties, un fichier de signature (FS) devra être ajouté à chaque partie du fichier.

- Pour créer votre fichier de signature vous devez utiliser le certificat digital qualifié (.pfx ou .p12) dont vous avez chargé la clé publique (.cer) sur le portail de la sécurité sociale lors de la création de votre canal SFTP.

- Un fichier de signature (FS) est obligatoire lors d'une déclaration dans l'environnement de production. Dans l'environnement de test et l'environnement simulation il n'est pas obligatoire de joindre un fichier de signature (FS). Si vous joignez un fichier de signature (FS) dans l'environnement de test ou de simulation, le fichier sera contrôlé.

Structure du nom du fichier de signature

FS.application.numéro d'expéditeur.date.le numéro d'ordre.l'environnement de travail.le nombre de parties.le numéro de la partie
Ex. FS.DMFA.123456.20120213.00001.T.1.1

(*) Vous trouverez les explications concernant la création d'un fichier de signature avec OpenSSL à la fin de ce manuel au point 10 Annexe: Générer un fichier de signature avec OpenSSL.

8.4 Le fichier GO

- Est un fichier vide.
- Est le signal que l'expéditeur a placé ses fichiers et que le traitement de ces fichiers peut commencer.
- Doit toujours être placé **après** les fichiers FI et FS comme dernier fichier dans le dossier **IN, INTEST** ou **INTEST-S**.
- Lors d'une déclaration en plusieurs parties (FI), un seul fichier GO est joint.

Pour créer un fichier GO, vous devez ouvrir un fichier vide (par exemple un fichier texte) et le sauvegarder sous le nom de fichier correct.

Structure du nom d'un fichier GO :

GO.application.numéro d'expéditeur.date.numéro de suite.environnement de travail.nombre de parties
Exemple : GO.DMFA.123456.20120213.00001.T.1

8.5 Le fichier TD

- Est un fichier vide.
- Sert à indiquer que les fichiers FI et/ou FS placés ne peuvent pas être traités (TD = To Delete). Un fichier TD peut donc être utilisé si les fichiers placés contiennent une erreur.
- Doit toujours être placé **après** les fichiers FI et FS comme dernier fichier dans le dossier **IN, INTEST** ou **INTEST-S**.
- Lors d'une déclaration en plusieurs parties (FI), un seul fichier TD est joint.
- Après l'envoi du fichier TD, l'expéditeur reçoit à titre de confirmation de la suppression un fichier ACRF avec **ResultCode 0**, **ErrorID ACRF-430** et la date et l'heure de la suppression sont ajoutées au nom du fichier.
  Ex. TD.DMFA.123456.20120213.00001.T.1_**20120213_102735**

Pour créer un fichier TD, vous devez ouvrir un fichier vide (par exemple un fichier texte) et le sauvegarder sous le nom de fichier correct.

Structure du nom d'un fichier TD :

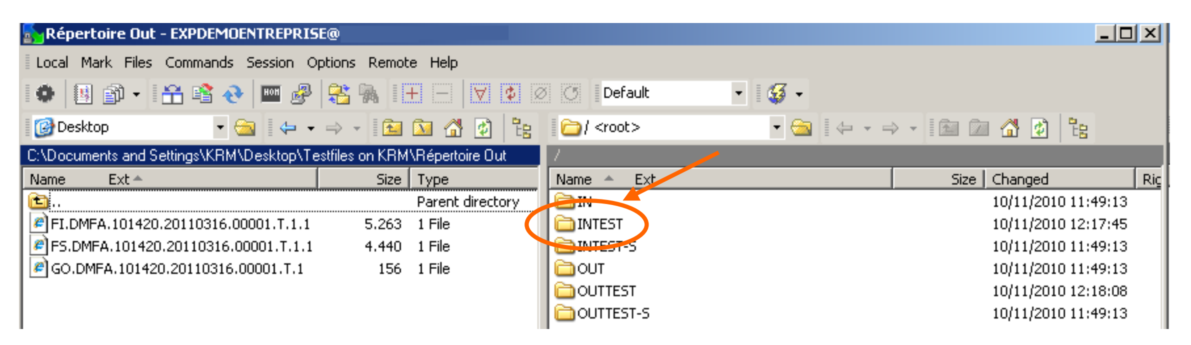
TD.application.numéro d'expéditeur.date.numéro de suite.environnement de travail.nombre de parties
Exemple : TD.DMFA.123456.20120213.00001.T.1

9. Transférer vos fichiers

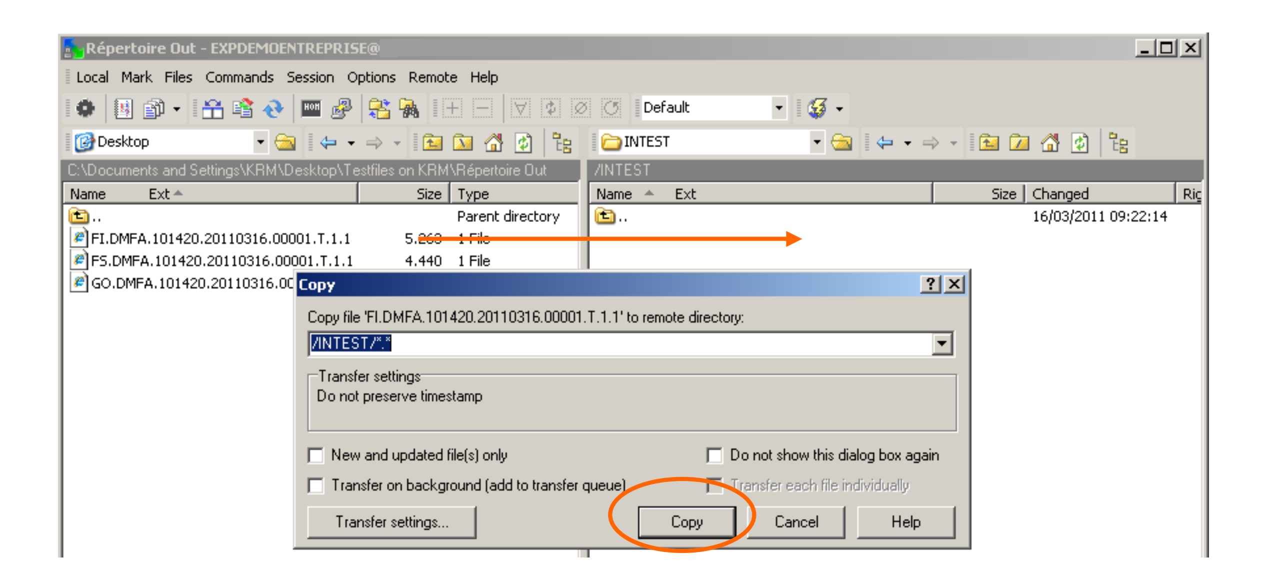
Ouvrez dans votre client SFTP le répertoire dans lequel vous souhaitez placer vos fichiers.

- Les fichiers de productions DmfA, DRS, Dimona, Chômage Temporaire, Déclaration Unique de Chantier (extension **R**) -> dans le répertoire **IN**
- Tests / fichiers de simulations DRS, Dimona, Chômage Temporaire, Déclaration Unique de Chantier et fichiers test de circuit DmfA (extension **T**) -> dans le répertoire **INTEST**
- Les fichiers test de déclaration DmfA (extension **S**) -> dans le répertoire **INTEST-S**

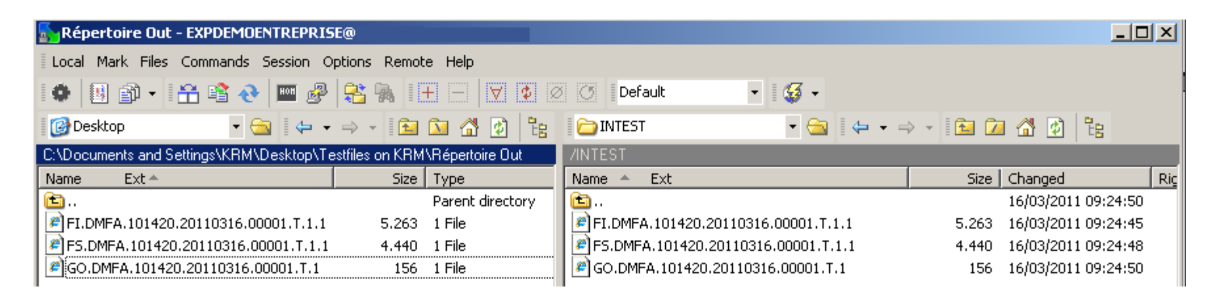
Dans cet exemple, nous allons ouvrir le répertoire INTEST pour déposer nos fichiers



Ensuite nous glissons les différents fichiers (FI, FS et GO) vers le répertoire INTEST. Comme le **fichier GO** lance le traitement toujours le glisser **en dernier** dans le répertoire.



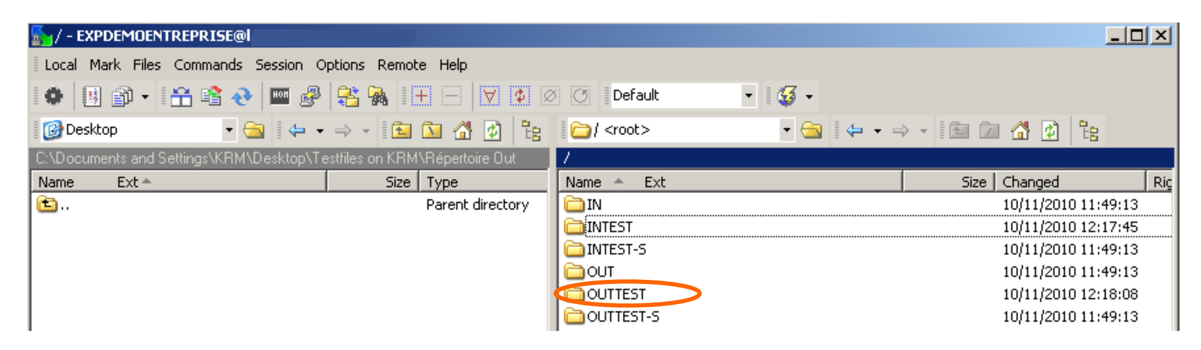
Dès que le **fichier GO** est placé, le traitement des fichiers liés démarre automatique.

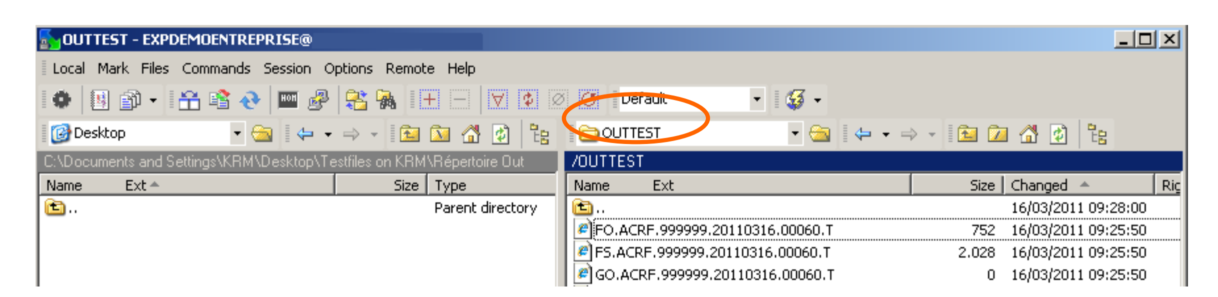


Dès que les déclarations sont traitées, vous retrouvez les réponses (ACRF, Notifications.) dans les répertoires respectifs :

- Les fichiers de productions DmfA, DRS, Dimona, Chômage Temporaire, Déclaration Unique de Chantier (extension **R**) -> dans le répertoire **OUT**
- Tests / fichiers de simulations DRS, Dimona, Chômage Temporaire, Déclaration Unique de Chantier et fichiers test de circuit DmfA (extension **T**) -> dans le répertoire **OUTTEST**
- Les fichiers test de déclaration DmfA (extension **S**) -> dans le répertoire **OUTTEST-S**

Nous ouvrons le répertoire OUTTEST

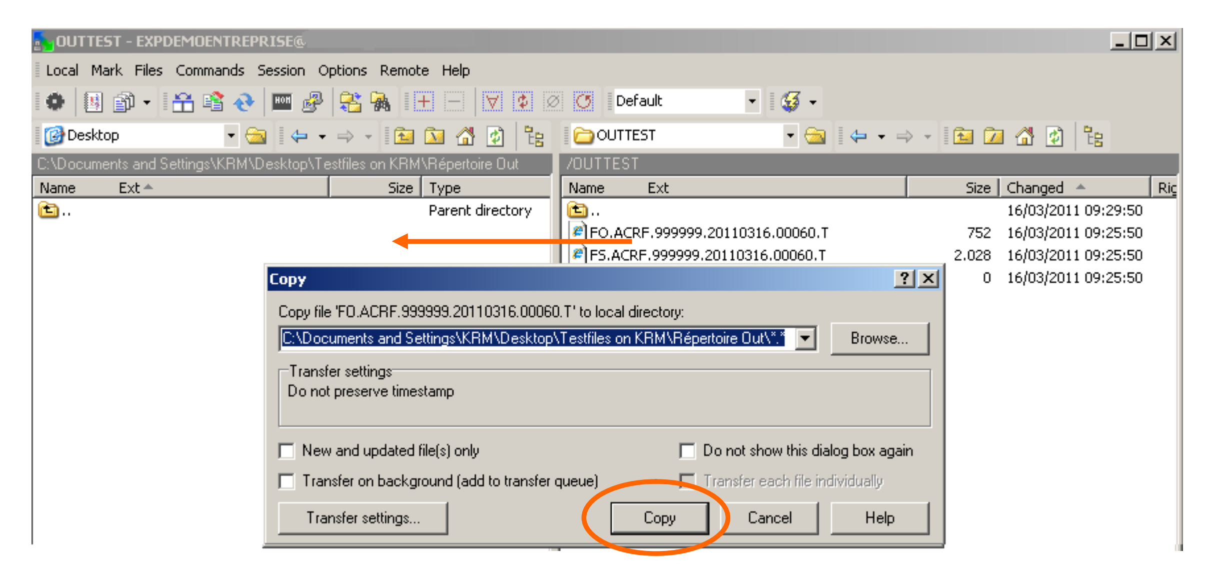




- Le récépissé ou ACRF est un message qui prouve que nous avons reçu votre fichier et que celui-ci répond aux conditions.

- Un récépissé positif signifie que votre fichier peut être traité. Dans ce cas, vous recevrez aussi une notification, plus tard, dans le même répertoire, avec le résultat du contrôle du contenu de votre déclaration.

Nous glissons les ACRF vers notre PC



Une fois que les fichiers ont été copiés sur notre ordinateur nous devons les supprimer sur le serveur SFTP.
Ensuite, les fichiers peuvent être ouverts et traités sur notre ordinateur même.



Gestion de vos répertoires OUT

Pour SFTP, les fichiers de réceptions sont mis à votre disposition dans les répertoires OUT, OUTTEST ou OUTTEST-S sur notre serveur.

Le but est que vous copiez les fichiers qui sont sur notre serveur vers un endroit sur votre PC. Ensuite, une fois copié, vous supprimez les fichiers des répertoires OUT sur notre serveur.

Etant donné que nous devons prévoir de l'espace pour tous les expéditeurs, nous ne pouvons pas garder les fichiers à disposition de manière indéterminée.

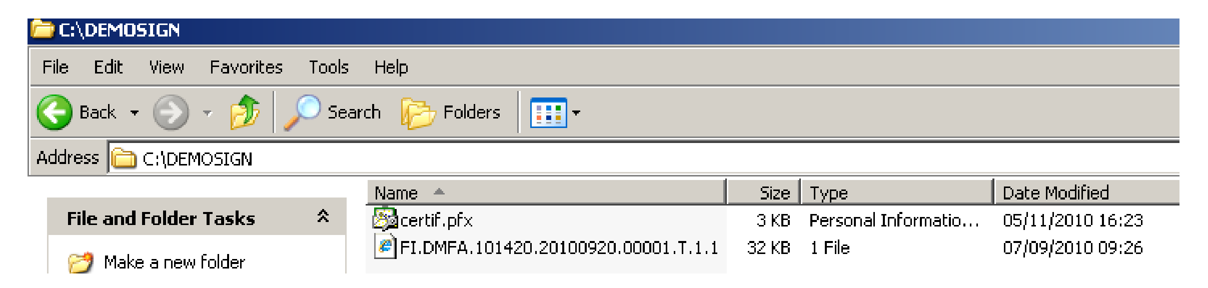
10. Annexe: Générer un fichier de signature avec OpenSSL :

Attention :

Cette procédure ne convient PAS aux certificats qui se trouvent sur une carte d'identité électronique (eID) ou une carte Isabel. Dans la pratique, cette procédure ne peut être utilisée que pour des certificats émis par Globalsign.

Pour créer un fichier de signature avec OpenSSL il faut d'abord installer ce software sur le PC sur lequel vous allez créer le fichier de signature.
Via un moteur de recherche, vous pouvez rechercher très simplement OpenSSL.

Après l'installation, le mieux est que vous fabriquiez un répertoire sur votre PC dans lequel vous installerez votre certificat (format .pfx place ou .p12) et votre fichier de déclaration (FI).



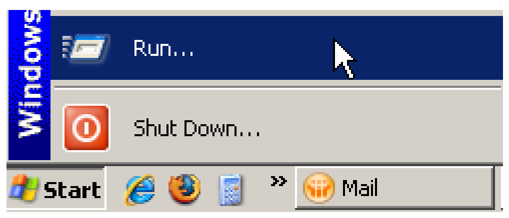
Nous expliquons ceci à l'aide d'un exemple :

- C:\DEMOSIGN : Le répertoire dans lequel se trouve le fichier de déclaration et le certificat
- certif.pfx: Nom de votre certificat
- ww123 : mot de passe du certificat
- ww789 : mot de passe que nous choisissons lors de la création de la clé

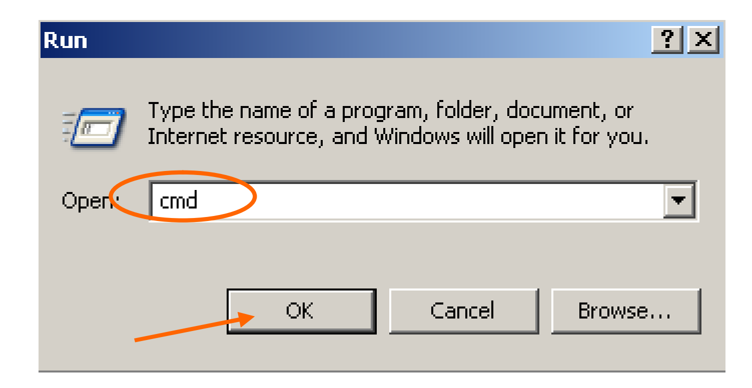
Nous allons créer un fichier .pem, un fichier .key et un fichier de signature (FS).
Nous choisissons dans notre exemple de donner le nom dmfa, au fichier .pem et au fichier .key. Cette dénomination est un libre choix. Vous pouvez choisir le nom vous-même et même si vous choisissez le nom dmfa vous pouvez l'utiliser pour signer les fichiers pour les autres applications.

Il est important de taper dans DOS les commandes correctes et les bons liens vers les répertoires.

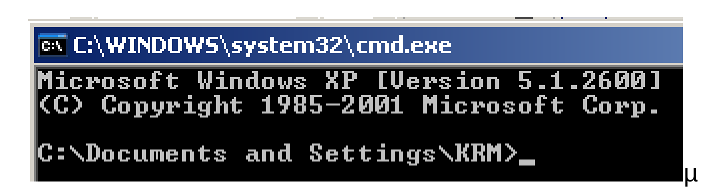
1. Ouvrez une fenêtre dos. Allez sur Start et cliquez sur **Run**



2.
3. Tapez **cmd** et cliquez sur ok



La fenêtre dos s'ouvre



µ

4. Ensuite vous devez aller vers C-prompt (c-à-d une ligne ou vous n'avez que '**C:\>**')
Pour y arriver vous devez taper plusieurs fois **cd..** suivi de la touche [ENTER]

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\KRM>**cd..**

C:\Documents and Settings>**cd**..

C:\>

5. Ouvrez le répertoire OpenSSL via la commande **cd openssl** puis cliquez sur [ENTER]

C:\>**cd openssl**

5. Ouvrez le sous-répertoire bin via la commande **cd bin** puis cliquez sur [ENTER]

```
C:\OpenSSL>cd bin
```

6. Ouvrez OpenSSL via la commande **openssl** puis cliquez sur [ENTER]

```
C:\OpenSSL\bin>openssl
```

Vous obtenez maintenant :

```
OpenSSL>
```

7. Vous pouvez maintenant créer **le fichier .pem**

Après ce prompt vous devez introduire la commande pour créer le fichier .pem. Attention, vous devez ici utiliser votre certificat format .pfx ou .p12 et non pas la clé publique du certificat (.cer).

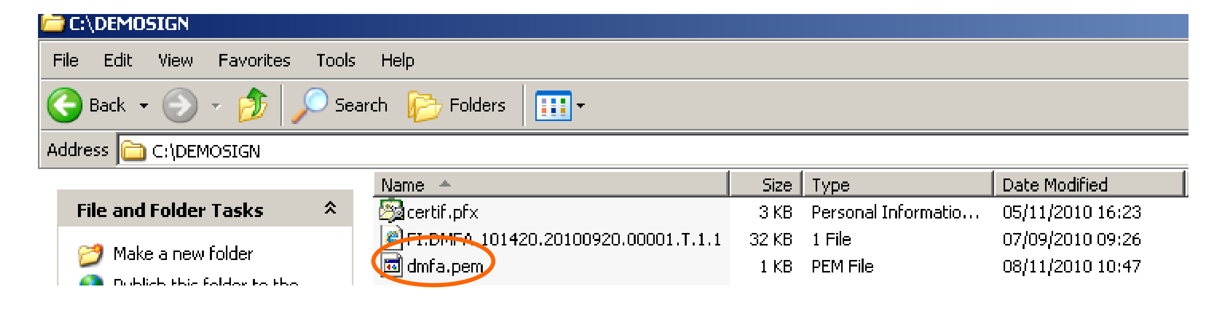
Vous introduisez la commande suivante avec le chemin complet du répertoire où se trouve le certificat et le fichier FI à signer :

pkcs12 -in Localisation de votre répertoire****votre certificat **-passin pass:** Mot de passe de votre certificat **-out** Localisation de votre répertoire****Nom de votre fichier.PEM-**clcerts -nokeys** puis cliquez sur [ENTER]

```
OpenSSL> pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 -out
C:\DEMOSIGN\dmfa.pem -clcerts -nokeys
```

Votre fichier.pem est créé et placé dans le répertoire où votre certificat et votre fichier de déclaration sont placés.

```
OpenSSL> pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 -out
C:\DEMOSIGN\dmfa.pem -clcerts –nokeys
MAC verified OK
```



8. Vous pouvez maintenant créer votre **fichier .key**

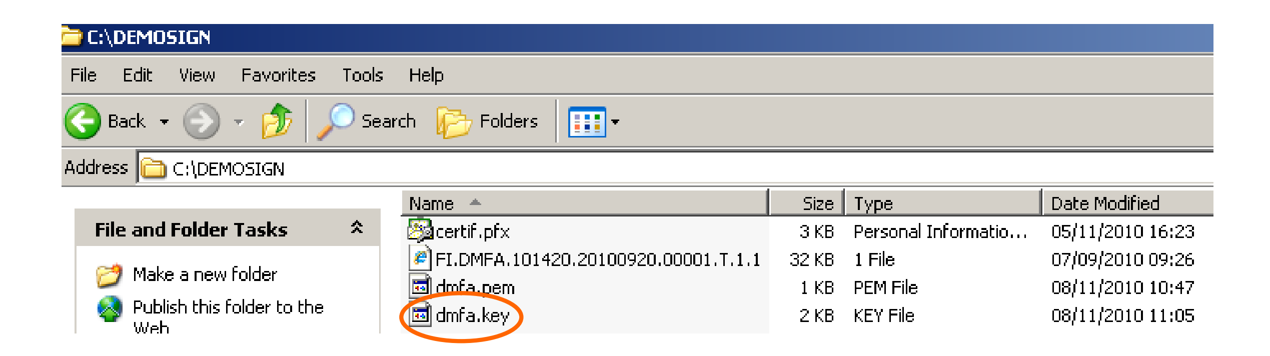
Vous introduisez la commande suivante dans le prompt OpenSSL :

pkcs12 -in Localisation de votre répertoire **** votre certificat**-passin pass:**Mot de passe de votre certificat**-passout pass:**mot de passe que vous choisissez pour votre .KEY **-out** Localisation de votre répertoire **** Nom de votre fichier.KEY puis cliquez sur [ENTER]

```
OpenSSL> pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 –passout
pass:ww789 -out C:\DEMOSIGN\dmfa.key
```

Votre fichier.key est créé et placé dans le répertoire où votre certificat, votre fichier de déclaration et votre fichier .pem sont placés.

```
OpenSSL> pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 –passout
pass:ww789 -out C:\DEMOSIGN\dmfa.key
MAC verified OK
```



Chaque fois que vous voulez envoyer un fichier FI, vous devez créer sur base du fichier FI avec les fichiers .pem et .key un fichier FS.

Vous pouvez utiliser les fichiers .pem et .key pendant toute la validité du certificat (voir Expiration Date de votre certificat). Une fois que votre certificat est périmé, vous devez charger un nouveau certificat pour le canal et vous devez créer des nouveaux fichiers .pem et .key.

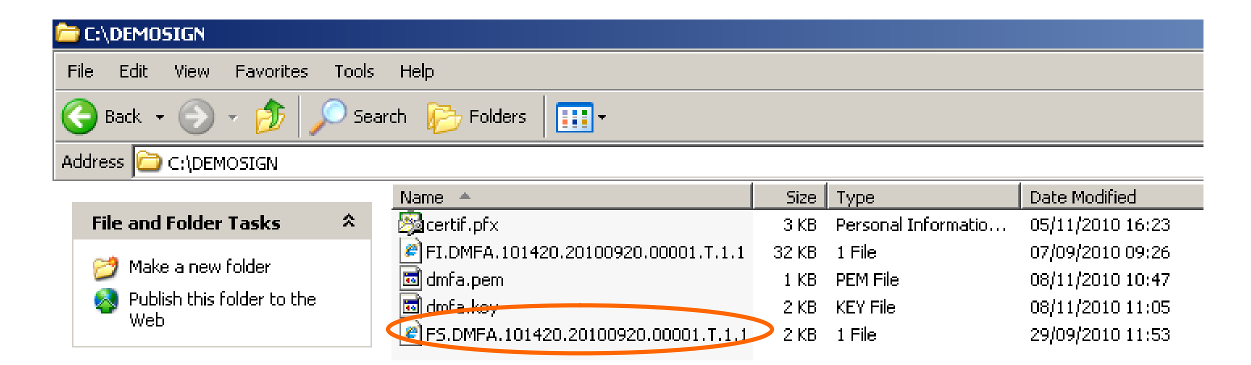
9. Vous pouvez maintenant créer votre **fichier de signature**

Le fichier FS peut être créé en introduisant les commandes suivantes dans le prompt OpenSSL :

smime -sign -in Localisation de votre répertoire****Nom du fichier FI **-signer** Localisation de votre répertoire****Nom de votre fichier .PEM **-inkey** Localisation de votre répertoire****Nom de votre fichier.KEY **-passin pass:** Mot de passe que vous avez choisi pour le .KEY **-outform PEM -out** Localisation de votre répertoire****Nom du fichier FS puis cliquez sur [ENTER]

OpenSSL> **smime -sign -in C:\DEMOSIGN\FI.DMFA.123456.20120213.00001.T.1.1 -signer C:\DEMOSIGN\dmfa.pem -inkey C:\DEMOSIGN\dmfa.key -passin pass:ww789 -outform PEM -out C:\DEMOSIGN\FS.DMFA.123456.20120213.00001.T.1.1**

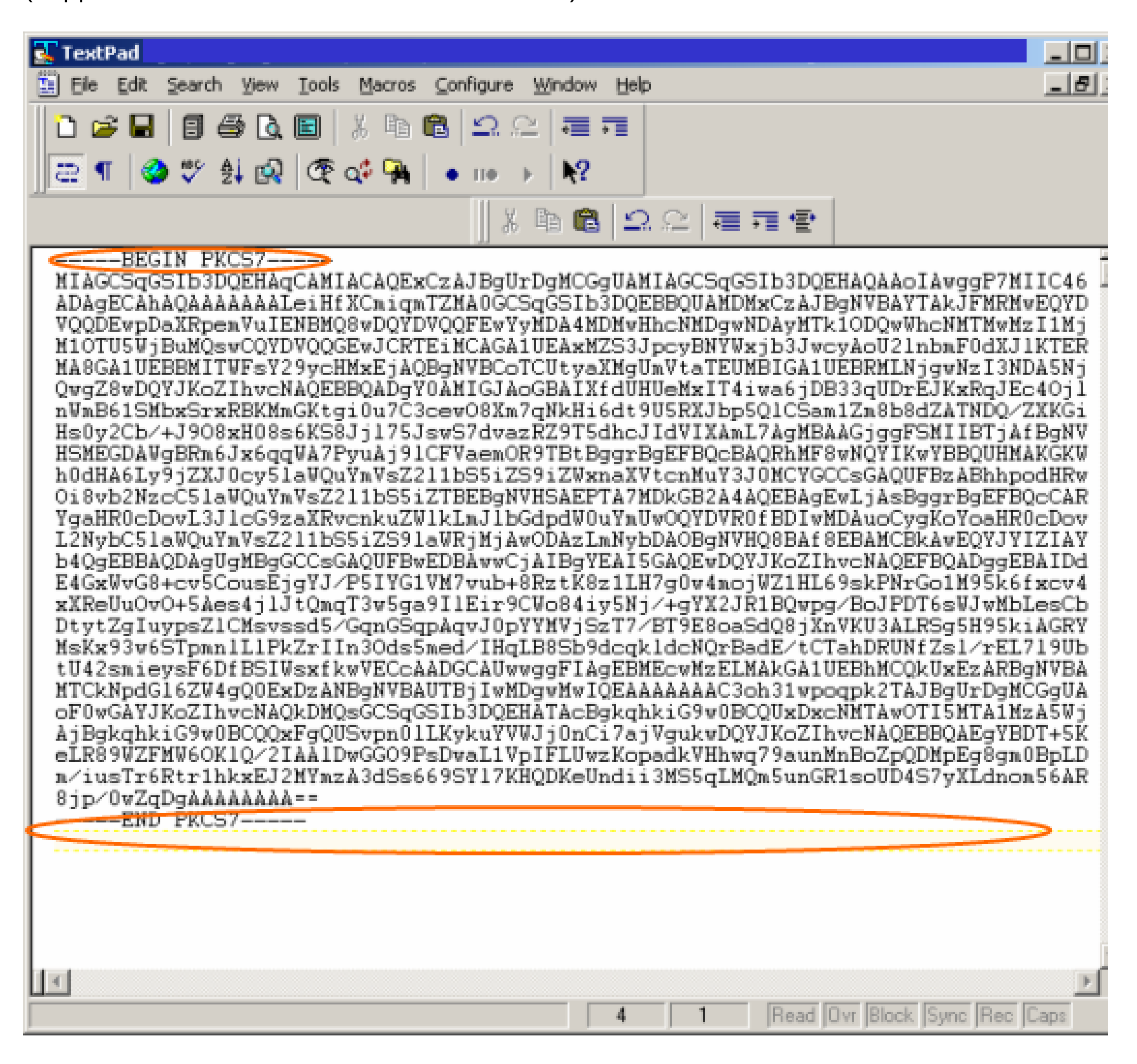
Votre fichier FS est créé dans le répertoire avec votre certificat et votre fichier de déclaration.



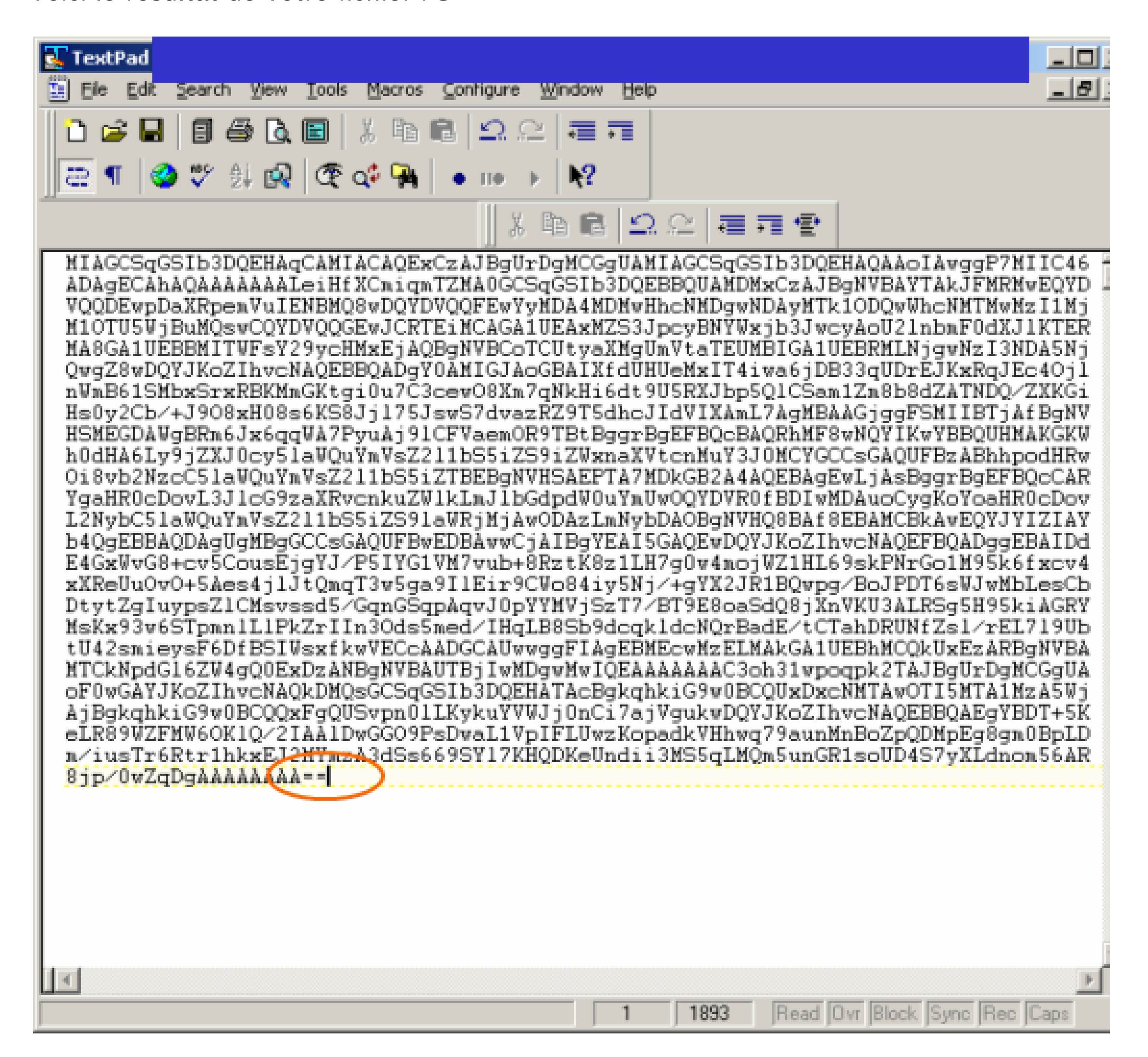
Attention: dès que vous avez créé votre fichier FS vous ne pouvez plus changer votre fichier FI. Si vous modifiez encore votre fichier FI vous devez recréer un nouveau fichier FS.

10. Les adaptations manuelles de votre fichier FS

Avant d'envoyer votre fichier, il y a encore quelques adaptations manuelles à faire dans le fichier FS.
Vous ouvrez le fichier FS avec un éditeur de texte comme Textpad ou Notepad.
Vous supprimez la première ligne (-----DÉBUT PKCS7-----) ainsi que la dernière ligne (-----END PKCS7-----).
Attention : le fichier FS ne peut pas contenir de lignes vierges à la fin du texte (supprimez éventuellement le retour chariot).



Voici le résultat de votre fichier FS



Après ces adaptations, sauvegardez le fichier FS avec la combinaison suivante [CTRL]+[S].

11. Questions

Vous envoyez en tant que (mandataire pour un) employeur affilié à l'ONSS.

Le centre de contact peut vous fournir de l'aide et des informations lors de l'ouverture de votre canal SFTP.

Accessible au:

(02/545.50.78

: batch@eranova.fgov.be

Heures d'ouverture :

- **De lundi jusqu'au vendredi, sauf les jours fériés**
- **Ouvert de 7h à 20h**

Vous envoyez en tant que (mandataire pour un) employeur affilié à l'ONSSAPL.

Votre gestionnaire de dossier à l'ONSSAPL peut vous fournir de l'aide et des informations lors de l'ouverture de votre canal SFTP. Vous pouvez également vous adresser au:

(02/239.14.07

: dmfappl@onssapl.fgov.be